REMARKS

The April 6, 2006 Office Action regarding the above-identified application has been carefully considered; and the amendments above together with the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action. The specification has been amended to correct grammar/spelling errors and to correct references to several of the drawings. The rejected claims have been replaced with a new set of claims, to patentably distinguish over art applied in the final Office Action. Care has been taken to avoid entry of new matter. For reasons discussed below, it is believed that this case is in condition for allowance. Prompt favorable reconsideration of this amended application is requested.

Summary of Disclosed Subject Matter

Before discussing the art rejection and distinctions of the new claims over the applied art, it may be helpful to consider the subject matter disclosed in the present application, both to show support for the new set of claims and to assist in understanding the distinctions of the claims over the art.

As disclosed by Applicants, a computer system in communication with the data applications of the wireless communication network facilitates user sign on to the data applications from the mobile station, by 'leveraging' authentication already performed by a network service control element or node, such as the Home Location Register or "HLR" (see e.g. paragraph [09]). The disclosed procedures effectively combine the authentication by the HLR with authentication by an Authentication, Authorization, and Accounting or "AAA" server. Traditional sign-on requirements to any particular data application, such as separate user ID and password verification are not required when the user of a previously authenticated mobile station attempts data application access via the wireless network. In other words, by leveraging the

authentication performed by the HLR, the AAA server need not separately authenticate a mobile station when a user attempts to access any particular data application. Since the HLR previously authenticated a mobile station, the same mobile station does not need to be re-authenticated when a user attempts to access a particular data application (see paragraph [36]). The leveraging may be implemented by periodically querying the HLR and storing identifications of HLR authenticated mobile stations in the AAA or by querying the HLR at the time of an attempt by the user to access a data application (see paragraph [37]). In either event, the AAA server checks for the existing successful HLR authentication so as to authenticate or prohibit access to a data application by a user accessing via a mobile station. Thus, instead of providing a username/password combination to the data application, the network takes advantage of mobile station identifiers which have been processed by the corresponding HLR in order to determine whether or not a mobile station and user is permitted to access a particular data application.

Although passwords may be used in some embodiments, the specification also suggests (e.g. in paragraph [69]) that from a mobile station, sign-on will be seamless, thus, not requiring a username/password. When the user attempts to access an application on a product server, the product server performs an authentication of the user in order to verify the identification of the user requesting service, by verifying the prior network validation. Basically, the product server sends the mobile station ID to the AAA server, which compares the mobile station identifier with authentication information leveraged from the HLR. If the identifier from the product server matches data for a mobile station that has already been successfully authenticated by the HLR, then the user is granted access to the data application service offered by that product server. In the event that the identifiers do not match, the product server may immediately terminate the

session, provide an information screen instructing the user to contact customer service, etc. Attention is directed to paragraphs [39] and [40] of the original specification.

As discussed in paragraph [41] of Applicants' specification, once a user has been authenticated, then the methodology provides a service authorization check. Two levels of authorization validation are described by way of example. First, basic authorization verifies that the user is authorized to use the service. Second, service type authorization determines the service type (i.e., class of service) to which the user has subscribed. Preferably, the AAA server performs both types of authorization, or separate AAA servers may perform each type, or selective AAA servers may perform authorization depending on the application the user attempts to access.

It is believed that the exemplary disclosure discussed above supports the recitations in the new set of claims 47-61 presented above and may also help with understanding of distinctions of the specific claim scope over the applied art, as will be discussed in more detail below.

Summary of the Art Rejection

The April 6, 2006 Office Action included a rejection of all of the prior claims under 35 U.S.C. § 102(e) as anticipated by US patent application publication number 2004/0225878 to Costa-Requena et al. (hereinafter the '878 publication). The '878 document discloses a technique facilitating generic authentication within an IP network. The disclosed system uses a plurality of network elements that employ different authentication protocols and a central authentication server 134 arranged to provide authentication service in response to received authentication requests from the various network elements (paragraph [0011]). For example, if authentication is requested from a WLAN access point, such as the RAS 142, the authentication server 134 receives information about the algorithm and protocol and will return the security

tokens formatted into the indicated protocol for that particular network element, such as the Extensible Authentication Protocol (EAP). Attention is directed to paragraph [0034].

The disclosed technique purportedly supports a 'single single sign-on' service in which, if a user has already authenticated himself with one service provider, the user need not authenticate himself with a second service provider. In the disclosed method, the sign-on at the first service provider lends itself to the second service provider, thus allowing the disclosed type of single sign-on. Attention is directed to paragraph [0050].

The rejection over the '878 publication is respectfully traversed on the ground that the technique disclosed in that publication does not in fact satisfy the requirements of the new claims submitted above. A more detailed explanation of the distinctions of the new claims over the '878 publication is set forth below.

Distinctions of the New Claims over the Art

New independent claim 47 relates to a method for managing authentication and authorization of user access to data applications of a service provider through a wireless communication network. Claim 47 includes requirements relating to both authentication and service authorization. The authentication relies on wireless network authentication of the mobile station, that is to say by a node of the wireless network, which in many cases eliminates the need for further authentication of the user by a server involved in providing the data application to the user. The authorization function involves validating that the authenticated user is actually authorized access to the particular data application or service.

The recited method involves authenticating a mobile station of a data application user as a valid mobile station for obtaining communication service through the wireless communication network, at a control node of the wireless communication network. Information is obtained from

the control node, which indicates successful authentication of the user's mobile station. When the user attempts to access a data application on a server through the wireless communication network, an identifier associated with the user is received and used to check the information to determine if there has been a successful authentication of the user's mobile station at the control node. If so, then the identifier is used to determine if the user is authorized to access the data application on the server, from among a number of data applications accessible through the wireless communication network. If authorized, then the method allows the user to access the data application on the server from the mobile station via communications through the wireless communication network.

It is respectfully submitted that the '878 publication does not suggest reliance on network validation of the user's mobile station as a user authentication for accessing a data application, in the manner recited in claim 47. In the '878 publication, an element requiring authentication implements the actual user authentication based on its own protocol, albeit using information supplied from the central authentication server. For example, if authentication is requested from a WLAN access point, such as the RAS 142, the authentication server 134 receives information about the algorithm and protocol and will return the appropriate security tokens to facilitate authentication through the RAS 142. Attention again is directed to paragraph [0034]. In such an arrangement, there is no use of an identifier associated with the data application user to check if there has been a successful authentication of the user's mobile station at a control node of the wireless communication network and attendant further processing if such prior authentication has occurred.

As noted, the '878 publication does mention support for a 'single sign-on' in which a sign-on at a first service provider lends itself to a second service provider (paragraph [0050]).

However, the limited disclosure on the point appears only to teach use of an additional 'liberty manager 324' to separate the message schemas from their associated profiles and bindings. It is respectfully submitted that this addition to the authentication server 434 disclosed in the '878 publication would not suggest to one of skill in the art a technique in which an identifier associated with the data application user is used to check if there has already been a successful authentication of the user's mobile station at control node of the wireless communication network and attendant further processing if such prior authentication has occurred.

It is further submitted that the '878 publication does not fairly suggest the recited authorization related steps. In the '878 publication, when the authentication service is operating on the network side, the authentication server provides the authentication service to a network element that is being accessed by a client, who must first be authenticated. In that case, the network element receives the attempt to access the network from a user supplying his own security credentials, and then forwards the credentials to the authentication server for validation. The authentication server will insure that the security credentials provided are correct according to the specific authentication protocol selected for the process (paragraph [0070]). However, it is not seen that the processing will further check user authorization to access the particular service, e.g. offered through the particular network element that received the attempt to access the network from the user. As such, the '878 publication does not satisfy the claim requirement for (after there has been a successful authentication of the user's mobile station at the control node of the wireless communication network) using the identifier to determine if the user is authorized to access the data application on the server, from among a plurality of data applications accessible through the wireless communication network, and if so allowing the user to access the data application on the server from the mobile station.

In view of the above-noted claim requirements not met by the '878 publication, it is believed that independent claim 47 is novel over that publication. Claims 48-56 depend from claim 47 and should be novel for at least the same reasons.

Claim 57 is a system claim. The recited system includes a wireless network, a control node for authenticating mobile stations of a data application user as a valid mobile station, a data application server, and an authentication and authorization server. Functions of the authentication and authorization server include obtaining from the control node information indicating successful authentication of the user's mobile station. The authentication and authorization server receives an identifier associated with the data application user from the data application server, when the user attempts to access the data application service on the data application server through the wireless communication network. In response to the identifier, the information is checked to determine if there has been a successful authentication of the user's mobile station at the control node of the wireless communication network. If so, then the authentication and authorization server also checks to determine if the user is authorized to access the data application on the server, from among the applications accessible through the wireless network. If the user is authorized, then the authentication and authorization server enables the data application server to permit the user to access the data application service from the mobile station via communications through the wireless communication network. It is respectfully submitted that the '878 publication does not disclose the recited system.

As discussed above, in the '878 publication, an element requiring authentication implements the actual user authentication based on its own protocol, albeit using information supplied from the central authentication server. It is not seen where the '878 publication suggests that an authentication and authorization server would determine if a network control

node such as the HLR has authenticated the mobile station, in the manner recited in claim 57. Applicants also submit that the '878 publication does not teach the subsequent check of authorization, before the authentication and authorization server enables the application server to allow the mobile station user to access the application service.

In view of the above-noted claim requirements not met by the '878 publication, it is believed that independent claim 57 is novel over that publication. Claims 58-61 depend from claim 57 and should be novel for at least the same reasons.

Conclusion

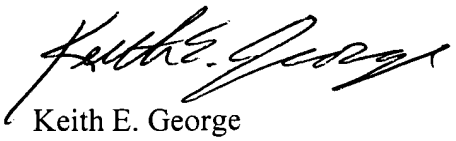
Upon entry of the above claim amendments, claims 47-61 are active in this application, all of which should be novel over the art applied in the Action. The art rejection from the last Office Action should be overcome. Applicants therefore submit that all of the claims are in condition for allowance. Accordingly, this case should now be ready to pass to issue; and Applicants respectfully request a prompt favorable reconsideration of this matter.

It is believed that this response addresses all issues raised in the April 6, 2006 Office Action. However, if any further issue should arise that may be addressed in an interview or by an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8603 KEG:apr
Facsimile: 202.756.8087
Date: August 7, 2006

Please recognize our Customer No. 20277 as our correspondence address.